A Swan-like Theorem

Antonia W. Bluher

February 1, 2008

Abstract

Richard G. Swan proved in 1962 that trinomials $x^{8k}+x^m+1 \in \mathbb{F}_2[x]$ with $8k > m$ have an even number of irreducible factors, and so cannot be irreducible. In fact, he found the parity of the number of irreducible factors for any square-free trinomial in $\mathbb{F}_2[x]$. We prove a result that is similar in spirit. Namely, suppose n is odd and $f(x) = x^n + \sum_{i\in S} x^i + 1 \in \mathbb{F}_2[x]$, where $S \subset \{i : i \text{ odd}, 0 < i < n/3\} \cup \{i : i = n \pmod 4, 0 < i < n\}$. We show that if $n = \pm 1 \pmod 8$ then f has an odd number of irreducible factors, and if $n = \pm 3 \pmod 8$ then f has an even number of irreducible factors. This has an application to the problem of finding polynomial bases $\{1, \alpha, \ldots, \alpha^{n-1}\}$ of $\mathbb{F}_{2^n}$ such that $\mathrm{Tr}(\alpha^i) = 0$ for all $1 \le i < n$.

1. Introduction

For purposes of implementing field arithmetic in $\mathbb{F}_{2^n}$ efficiently, it is desirable to have an irreducible polynomial $f(x) \in \mathbb{F}_2[x]$ of degree n with as few terms as possible. The number of terms must be odd, as otherwise $x+1$ would be a factor. Often a trinomial x^n+x^m+1 can be found, or at least a pentanomial, $x^n+x^{m_1}+x^{m_2}+x^{m_3}+1$, where $n > m_1 > m_2 > m_3 > 0$. If α is a root of f, then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $\mathbb{F}_{2^n}/\mathbb{F}_2$, called a *polynomial basis*. Multiplication with respect to this basis is more efficient when the number of terms in f is small. In addition, multiplication will be more efficient if f has the form $x^n + g(x)$, where $\deg(g)$ is small. For a trinomial, we would like m to be small, and for a pentanomial, we would like m_1 to be small.

It is also desirable to be able to compute the trace quickly. Now $\mathrm{Tr}(\sum a_i\alpha^i) = \sum_{i\in I} a_i$, where $I = \{i : \mathrm{Tr}(\alpha^i) = 1\}$. Thus, trace is especially easy to compute if I has a single element. Ahmadi and Menezes [1] showed that if n is odd, then $|I| = 1$ if and only if $f(x)+1$ contains only monomials of odd degree. They computed irreducible trinomials and pentanomials with this property (m odd for a trinomial, and $m_1m_2m_3$ odd for a pentanomial.) To their surprise, m_1 seemed to be always small when $n = \pm 1 \pmod 8$, but $m_1 \ge n/3$ when $n = \pm 3 \pmod 8$. This article explains their observation: we prove that if $n = \pm 3 \pmod 8$ and $m_1 < n/3$, then $x^n + x^{m_1} + x^{m_2} + x^{m_3} + 1$ has an *even* number of irreducible factors, and so it cannot be irreducible. More generally, we prove:

Theorem. *Let n be odd and $f(x) = x^n + \sum_{i\in S} x^i + 1 \in \mathbb{F}_2[x]$, where*

$$S \subset \{\, i : i \text{ odd}, 0 < i < n/3 \,\} \cup \{\, i : i = n \pmod 4, 0 < i < n \,\}. \tag{1}$$

Then f has no repeated roots. If $n = \pm 1 \pmod 8$ then f has an odd number of irreducible factors. If $n = \pm 3 \pmod 8$ then f has an even number of irreducible factors.

The bound $n/3$ is sharp, as shown by the example $x^{21} + x^7 + 1$, which is irreducible.

Corollary 1.1 *Let $n = \pm 3 \pmod 8$ and let $f \in \mathbb{F}_2[x]$ be an irreducible polynomial of degree n such that $\mathrm{Tr}(\alpha^i) = 0$ for each $1 \leq i < n$. Then $f(x)$ contains a term x^k with $n > k \geq n/3$.*

Proof. Ahmadi and Menezes [1] showed that all the terms occurring in $f + 1$ have odd exponent. Let $f = x^n + x^k +$ lower degree terms. By the theorem, f will have an even number of irreducible factors unless $k \geq n/3$. ∎

Our theorem is closely related to work of Fredricksen, Hales, and Sweet [2]. The first theorem in their paper, when specialized to $g(x) = 1 + \sum_{i \text{ odd}} a_i x^i$, yields a weak form of this theorem, namely that for n odd and $n > 5\deg(g)$, the parity of the number of factors of $x^n + g(x)$ is a periodic function of n, with period 8.

2. Resultants and discriminants

This section gives background on resultants which will be needed for the proof of the theorem. An excellent reference is [5, Sections 5.8 and 5.9].

Let $f = \sum_{i=0}^{n} a_i x^{n-i}$ and $g = \sum_{i=0}^{m} b_i x^{m-i}$ be polynomials in $K[x]$, where K is a field and $a_0 b_0 \neq 0$. The resultant of f and g, denoted $R(f, g)$, is the determinant of the matrix

$$\begin{pmatrix}
a_0 & a_1 & a_2 & \dots & a_n & & & \\
 & a_0 & a_1 & a_2 & \dots & a_n & & \\
 & & & \dots & & & & \\
 & & & a_0 & a_1 & a_2 & \dots & a_n \\
b_0 & b_1 & b_2 & \dots & b_m & & & \\
 & b_0 & b_1 & b_2 & \dots & b_m & & \\
 & & & & \dots & & & \\
 & & & & b_0 & b_1 & \dots & b_m
\end{pmatrix}. \tag{2}$$

Here there are m rows containing coefficients of f and n rows containing coefficients of g, and the principal diagonal contributes $a_0^m b_m^n$ to the determinant. Now f, g can be factored completely into linear factors over the algebraic closure:

$$\begin{aligned} f(x) &= a_0(x - x_1)(x - x_2)\cdots(x - x_n) \\ g(x) &= b_0(x - y_1)(x - y_2)\cdots(x - y_m). \end{aligned}$$

As shown in [5],

$$R(f, g) = a_0^m \prod_{i=1}^{n} g(x_i) = (-1)^{mn} b_0^n \prod_{j=1}^{m} f(y_j).$$

The resultant respects the following properties.

(R1) If $g = fq + r$, $R(f, g) = R(f, r)$.

(R2) $R(x,g) = g(0)$, $R(f,-x) = f(0)$.

(R3) $R(f_1 f_2, g) = R(f_1,g)R(f_2,g)$, $R(f, g_1 g_2) = R(f,g_1)R(f,g_2)$.

Note that $R(f,g) = 0$ if and only if f vanishes at a root of g in $\overline{K}$; equivalently, if and only if $\mathrm{GCD}(f,g)$ has degree ≥ 1. Also, if the coefficients of f, g belong to a subring $A \subset K$, then $R(f,g) \in A$. We will apply this to the case $\mathbf{Z} \subset \mathbf{Q}$; thus $R(f,g) \in \mathbf{Z}$ is defined for $f, g \in \mathbf{Z}[x]$. It will be handy to note that if $a_0 = 1$ then we can pad $g(x)$ with leading zeros (thereby increasing m and allowing $b_0 = 0$) without affecting the determinant of the above matrix.

If $f = (x - x_1) \cdots (x - x_n)$ then

$$R(f,f') = \prod_i f'(x_i) = \prod_{i \neq k} (x_i - x_k) = (-1)^{n(n-1)/2} \prod_{i<k} (x_i - x_k)^2.$$

The *discriminant* of f is defined as

$$\mathrm{disc}(f) = \prod_{i<j} (x_i - x_j)^2 = (-1)^{n(n-1)/2} R(f,f').$$

Swan [4, Corollary 3] proved the following:

Stickelberger-Swan Theorem. *Let $f \in \mathbb{F}_2[x]$, and suppose* $\mathrm{disc}(f) \neq 0$ *(equivalently, f has no repeated roots). Let t denote the number of irreducible factors of $f(x)$ over $\mathbb{F}_2[x]$. Let $F(x) \in \mathbf{Z}[x]$ be any monic lift to the integers. Then $t = \deg(f) \pmod 2$ if and only if $\mathit{disc}(F) = 1 \pmod 8$.*

Swan used this result to characterize the square-free trinomials in $\mathbb{F}_2[x]$ which have an odd number of irreducible factors. A characterization for tetranomials in $\mathbb{F}_2[x]$ was recently obtained by Hales and Newhart [3]. Another very interesting generalization of Swan's Theorem is given by Fredricksen, Hales, and Sweet [2].

3. Proof of the theorem

Let F be the lift of f to $\mathbf{Z}$ which has all its coefficients equal to 0 or 1, that is,

$$F(x) = x^n + \sum_{i \in S} x^i + 1 \in \mathbf{Z}[x]. \tag{3}$$

We will show $\mathrm{disc}(F) = 1 \pmod 8$ if $n = \pm 1 \pmod 8$ and $\mathrm{disc}(F) = 5 \pmod 8$ if $n = \pm 3 \pmod 8$. Since $\mathrm{disc}(f) = \mathrm{disc}(F) \pmod 2$, this will imply f has nonzero discriminant, hence distinct roots. Further, the Stickelberger-Swan Theorem will imply that f has an odd number of irreducible factors if and only if $n = \pm 1 \pmod 8$.

We compute $\mathrm{disc}(F)$ using the properties of discriminants and resultants given in Section 2. We have

$$\mathrm{disc}(F) = (-1)^{n(n-1)/2} R(F,F').$$

Since $R(F,-x) = F(0) = 1$, we have $R(F,F') = R(F,-xF') = R(F,-xF' + nF)$, and so

$$n^n \mathrm{disc}(F) = (-1)^{n(n-1)/2} R(F,G), \qquad \text{where } G = n(nF - xF').$$

Now

$$G = \sum_{i \in S} n(n-i)x^i + n^2 = 4G_4(x) + 2G_2(x) + 1 \pmod 8,$$

where

$$\begin{aligned} G_2(x) &= \sum_{i \in S,\ n-i=2 \pmod 4} \left(\frac{n(n-i)}{2}\right) x^i, \\ G_4(x) &= \sum_{i \in S,\ n-i=4 \pmod 8} \left(\frac{n(n-i)}{4}\right) x^i. \end{aligned}$$

Note that $\deg(G_2) < n/3$ and $\deg(G_4) < n$ by (1). We will prove that

$$R(F, G) = 1 \pmod 8.$$

This will imply $n^n \mathrm{disc}(F) = (-1)^{n(n-1)/2} \pmod 8$. Since $n^2 = 1 \pmod 8$ we conclude $\mathrm{disc}(F) = n(-1)^{n(n-1)/2} \pmod 8$, and this equals 1 if $n = \pm 1 \pmod 8$, or 5 if $n = \pm 3 \pmod 8$, as required.

It remains to prove $R(F, G) = 1 \pmod 8$. Since we are allowed to pad G with leading zeros (as explained in Section 2), we may assume $\deg(G) = n-4$. Now set up the corresponding matrix for the resultant. Lemma 4.4 below implies that this matrix has determinant 1 (mod 8). This completes the proof of the theorem.

Unfortunately, Lemma 4.4 is technical and unenlightening. For this reason, we include two simpler lemmas which imply special cases of the theorem. Namely, Eq (4) of Lemma 4.2 (with $F_0 = F_1 = 0$) implies our result when $S \subset \{\, i \ odd : 0 < i < n/3 \,\}$, and Eq (5) handles the case when $S \subset \{\, i : i = n \pmod 4, i < n/2 \,\}$. Lemma 4.3 implies $R(F, G) = 1 \pmod 8$ when $S \subset \{\, i : i = n \pmod 4, 0 < i < n \,\}$.

4. Some lemmas

In this section we provide the lemmas which were promised at the end of the preceding section. Lemmas 4.2 and 4.3 can be used to show $R(F, G) = 1 \pmod 8$ in special cases, and Lemma 4.4 handles the general case.

Lemma 4.1 *Let D be a square matrix with entries in $\mathbf{Z}/8\mathbf{Z}$ such that D_{ij} is even and $D_{ij}D_{ji} = 0$ whenever $i \neq j$. Then* $\det(D) = \prod D_{ii}$.

Proof. Consider the expansion of $\det(D)$. The principal diagonal contributes $\prod_{i=1}^n D_{ii}$. We claim all other terms are 0 mod 8. Indeed, a nonprincipal summand contains some D_{ij} with $i \neq j$. If it also contains D_{ji} then the summand is 0 (mod 8). If not then the summand contains some $D_{j\ell}$ from the jth row and D_{ki} from the ith column, where i, j, k and i, j, ℓ are distinct; but in that case the summand is again 0 (mod 8) since it contains the product of at least three off-diagonal entries. ∎

Lemma 4.2 *Let $H \in \mathbf{Z}[x]$, $x|H$, and* $\deg(H) = s$. *Let $n > 1$ and $F_0, F_1, F_2 \in \mathbf{Z}[x]$ such that* $\deg(F_k) < n - ks$, $k = 0, 1, 2$. *Then*

$$R(x^n + 4F_0(x) + 2F_1(x) + F_2(x), 2H + 1) = 1 \pmod 8 \tag{4}$$

$$R(x^n + 2F_0(x) + F_1(x), 4H + 1) = 1 \pmod 8. \tag{5}$$

Proof. First we prove (4). The resultant $R(x^n + 4F_0(x) + 2F_1(x) + F_2(x), 2H(x) + 1)$ is the determinant of an $(n+s) \times (n+s)$ matrix of a special shape; we will take advantage of this to show that its determinant is 1 (mod 8). For example, in the case $s = 3$, $n = 12$ the matrix looks like:

$$\begin{pmatrix}
\mathrm{I} & 4 & 4 & 4 & 2 & 2 & 2 & * & * & * & * & * & * & 0 & 0 \\
0 & \mathrm{I} & 4 & 4 & 4 & 2 & 2 & 2 & * & * & * & * & * & * & 0 \\
0 & 0 & \mathrm{I} & 4 & 4 & 4 & 2 & 2 & 2 & * & * & * & * & * & * \\
2 & 2 & 2 & \mathrm{I} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 2 & 2 & 2 & \mathrm{I} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 2 & 2 & \mathrm{I} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 2 & 2 & 2 & \mathrm{I} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & & & & & & & \ldots & & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & \mathrm{I}
\end{pmatrix}$$

where I denotes an integer which is 1 (mod 8), $*$ denotes any integer, 2 denotes any even integer, 4 denotes any integer which is divisible by 4, and 0 denotes any integer which is divisible by 8. There are s 4's, s 2's, and $(n-2s)$ *'s in each of the first s rows. Let M denote this matrix, and $\overline{M}$ its image in $\mathbf{Z}/8\mathbf{Z}$. Since $\det(\overline{M}) = \det(M) \pmod 8$, it suffices to consider the entries as belonging to $\mathbf{Z}/8\mathbf{Z}$.

Use the 1's in the first s rows as pivots to clear the even numbers in the columns below them to obtain a matrix of the form:

$$\begin{pmatrix}
\mathrm{I} & 4 & 4 & 4 & 2 & 2 & 2 & * & * & * & * & * & * & 0 & 0 \\
0 & \mathrm{I} & 4 & 4 & 4 & 2 & 2 & 2 & * & * & * & * & * & * & 0 \\
0 & 0 & \mathrm{I} & 4 & 4 & 4 & 2 & 2 & 2 & * & * & * & * & * & * \\
0 & 0 & 0 & \mathrm{I} & 4 & 4 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
0 & 0 & 0 & 2 & \mathrm{I} & 4 & 4 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
0 & 0 & 0 & 2 & 2 & \mathrm{I} & 4 & 4 & 4 & 2 & 2 & 2 & 2 & 2 & 2 \\
0 & 0 & 0 & 2 & 2 & 2 & \mathrm{I} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 2 & 2 & 2 & \mathrm{I} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & \mathrm{I} & 0 & 0 & 0 & 0 & 0 & 0 \\
 & & & & & & & & \ldots & & & & & & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & \mathrm{I}
\end{pmatrix}$$

This matrix has the form $\overline{M} = \left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)$, where A is upper-triangular with 1's on the diagonal and D has 1's on the diagonal and satisfies the conditions of Lemma 4.1. Hence, $\det(\overline{M}) = \det(A)\det(D) = 1$.

The equation (5) is proved similarly, except that one begins with a matrix of the form

$$\begin{pmatrix}
\mathrm{I}\ 2\ 2\ 2\ *\ *\ *\ *\ *\ *\ *\ *\ *\ 0\ 0 \\
0\ \mathrm{I}\ 2\ 2\ 2\ *\ *\ *\ *\ *\ *\ *\ *\ *\ 0 \\
0\ 0\ \mathrm{I}\ 2\ 2\ 2\ *\ *\ *\ *\ *\ *\ *\ *\ * \\
4\ 4\ 4\ \mathrm{I}\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\
0\ 4\ 4\ 4\ \mathrm{I}\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\
0\ 0\ 4\ 4\ 4\ \mathrm{I}\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\
0\ 0\ 0\ 4\ 4\ 4\ \mathrm{I}\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\
\multicolumn{15}{c}{\cdots} \\
0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 4\ 4\ 4\ \mathrm{I}\ 0 \\
0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 4\ 4\ 4\ \mathrm{I}
\end{pmatrix}.$$

∎

If $F = x^n + \sum_{i \in S} x^i + 1$ with $S \subset \{\, i \text{ odd} : 0 < i < n/3 \,\}$ then we can apply Eq. (4) to show $R(F,G) = 1 \pmod 8$, taking $F_0 = F_1 = 0$, $F_2 = \sum_{i \in S} x^i + 1$, $H = G_2 + 2G_4$. If $S \subset \{\, i : i = n \pmod 4, 0 < i < n/2 \,\}$ then we apply Eq. (5) with $F_0 = 0$, $F_1 = \sum_{i \in S} x^i + 1$, $H = G_4$. For the case $S \subset \{\, i : i = n \pmod 4, 0 < i < n \,\}$ one verifies that the matrix M which computes $R(F,G)$, when reduced mod 8, satisfies the conditions of Lemma 4.3 below, and so $R(F,G) = \det(M) = 1 \pmod 8$. For the general case of S as in (1), we require the more complicated Lemma 4.4 in order to show $R(F,G) = 1 \pmod 8$.

Lemma 4.3 *Let $0 \le m < n$ and let M be an $(m+n) \times (m+n)$ matrix with entries in $\mathbf{Z}/8\mathbf{Z}$ of the form:*

$$\begin{pmatrix} A & B \\ C & \\ 0 & D \end{pmatrix}$$

where $A = (a_{ij}), C = (c_{ij})$ are $m \times m$ matrices, $B = (b_{i\ell})$ is $m \times n$, $D = (d_{k\ell})$ is $n \times n$. Assume the following conditions hold:

1. *The principal diagonal entries of M are all equal to 1 (i.e., $a_{ii} = d_{kk} = 1$ for $1 \le i \le m$ and $1 \le k \le n$).*
2. *A is upper-triangular, and a_{ij} is even when $i + j$ is odd.*
3. *C is upper-triangular, all entries of C are divisible by 4, and $c_{ij} = 0$ when $i + j$ is odd.*
4. *$d_{k\ell} = 0 \pmod 4$ when $k \ne \ell$.*
5. *b_{ir} is even when $r \le i$ and $i + r$ is even.*

Then $\det(M) = 1 \pmod 8$.

Proof. Since A is upper-triangular with 1's on its principal diagonal, the top m rows of M may be used as pivots. Because of the conditions on C, a row operation will consist of adding four times the i-th row of $(A\ B)$ onto the rth row of $\binom{C}{0}\ D)$, where $r \le i$ and $r = i \pmod 2$. After each pivot operation, the conditions on C will remain true: the entries of C will still be

divisible by 4, and c_{rs} will still be 0 when $r+s$ is odd because a_{is} is even when $i+s$ is odd. The conditions on D will also remain true: d_{rr} will still be one because b_{ir} is even. After completing the pivot operations, C will be reduced to 0. Thus, $\det(M) = \det(A)\det(D)$. Clearly $\det(A) = 1$, and $\det(D) = 1$ by Lemma 4.1. ∎

The next lemma implies $R(F,G) = 1$ in the general case where S is as in (1). Here F, G have the form

$$\begin{aligned} F(x) &= x^n + \sum_{\substack{4|k \\ 0<k<n}} a_k x^{n-k} + \sum_{\substack{k=2 \pmod 4 \\ (2n/3)<k<n}} a_k x^{n-k} + 1 \\ G(x) &= 4\sum_{\substack{4|k \\ 0<k<n}} b_k x^{n-k} + 2 \sum_{\substack{k=2 \pmod 4 \\ (2n/3)<k<n}} b_k x^{n-k} + 1 \end{aligned}$$

where $a_k, b_k \in \mathbf{Z}$. We consider G to have degree $m = n-4$ (possibly with leading zeroes) and set up the matrix M which computes the resultant $R(F,G)$. This matrix, when reduced mod 8, satisfies the conditions of the next lemma, so $R(F,G) = \det(M) = 1 \pmod 8$. The proof of Lemma 4.4 is similar to that of Lemma 4.3, but the details are much messier.

Lemma 4.4 *Let $n \geq 5$ be odd, $m = n-4$, and $M = \binom{X}{Y}$ be a square matrix over $\mathbf{Z}/8\mathbf{Z}$, where X is $m \times (m+n)$ and Y is $n \times (m+n)$. Let $s = \lfloor (n-1)/3 \rfloor$. Assume*

(H1) $M_{ii} = 1$ for $1 \leq i \leq n+m$; equivalently, $X_{ii} = Y_{r,r+m} = 1$ for $1 \leq i \leq m$ and $1 \leq r \leq n$.

(H2) $X_{ij} = 0$ unless $j - i \in ([0, n-s) \cap 4\mathbf{Z}) \cup ([n-s, n) \cap 2\mathbf{Z}) \cup \{n\}$.

(H3) $Y_{ij} = 0$ if $j < i$, and Y_{ij} is even if $j \neq m+i$.

(H4) For $k \in [0, m-s)$, we have

$$Y_{i,i+k} = \begin{cases} 0 \pmod 4 & \text{if } k = 0 \pmod 4 \\ 0 \pmod 8 & \text{otherwise.} \end{cases}$$

(H5) For $k \in [m-s, m+n-2s)$ and $k \neq m$, we have

$$Y_{i,i+k} = \begin{cases} 0 \pmod 2 & \text{if } k = 2 \pmod 4, \\ 0 \pmod 4 & \text{if } k = 0 \pmod 4, \text{ or if } k \text{ is odd and } i+k > m, \\ 0 \pmod 8 & \text{otherwise.} \end{cases}$$

Then $\det(M) = 1 \bmod 8$.

Proof. Write $X = (A\ B)$, where A is $m \times m$. By hypothesis, A is an upper-triangular matrix with 1's on the diagonal, and so the rows of X may be used as pivots to clear the first m columns of Y. We will show below that the new Y still satisfies the hypotheses, but with the first m columns of Y equal to 0. Let D denote the rightmost n columns of Y; then $\det(M) = \det(D)$. We will show below that $\det(D) = 1$.

It remains to prove the two claims: (1) when a row of X is used as a pivot to clear the first m columns, the new matrix still satisfies the hypotheses; and (2) $\det(D) = 1$.

We begin with the second claim. We show that D has 1's on the diagonal and satisfies the hypotheses of Lemma 4.1. By (H1) and (H3), the diagonal entries D_{ii} are equal to 1, and the off-diagonal entries are even. We now show $D_{ij}D_{ji} = 0 \pmod 8$ if $i \neq j$. By symmetry we can assume $i < j$. Since D_{ij} and D_{ji} are even, it suffices to show one of D_{ij}, D_{ji} is $0 \pmod 4$. Assume 4 does not divide D_{ji} and we will show that 4 divides D_{ij}. Let $t = j - i > 0$. Then $D_{ij} = Y_{i,i+(m+t)}$, $D_{ji} = Y_{j,j+(m-t)}$. Since 4 does not divide D_{ji}, (H4) implies that $m-t$ is not in $[0, m-s)$. By (H3), $m - t \geq 0$. Thus, $m - t \geq m - s$, and so $0 < t \leq s$. Then, $(m-t)$ is in $[m-s, m)$. By (H5), $m - t = 2 \pmod 4$. Then t is odd, so $2t = 2 \pmod 4$. Thus, $m + t = (m-t) + 2t = 0 \pmod 4$. Further, $m + t$ lies in the interval $(m, m+s]$, so by (H5), $D_{ij} = 0 \pmod 4$. We conclude that $D_{ij}D_{ji} = 0 \pmod 8$. Thus, $\det(D) = 1$ by Lemma 4.1.

Now we verify the first claim. Consider a nonzero entry in the leftmost m columns of Y, say $e = Y_{ri} \neq 0$, where $i \leq m$. To clear this entry, we subtract e times the i^{th} row of X from the r^{th} row of Y. Let Y' denote the new matrix, thus $Y'_{r's} = Y_{r's}$ if $r' \neq r$ and

$$Y'_{rs} = Y_{rs} - eX_{is}, \qquad e = Y_{ri}.$$

We must check that if the hypotheses hold for X and Y then they also hold for X and Y'. The hypotheses will certainly hold for Y'_{rs} if $eX_{is} = 0$, so we may assume $eX_{is} \neq 0$.

Let $k = i - r$, and note that $k < i \leq m$. We have $e = Y_{r,r+k} \neq 0$. By (H3), $k \geq 0$. Since $0 \leq k < m$ and $k + r = i \leq m$, (H4) and (H5) imply one of the following holds:

$$0 \leq k < m,\ 4|k,\ 4|e \qquad or \qquad m - s \leq k < m,\ k = 2 \bmod 4,\ e \text{ is even.} \tag{6}$$

Let $k' = s - r$. The equation $Y'_{rs} = Y_{rs} - eX_{is}$ can be rewritten as

$$Y'_{r,r+k'} = Y_{r,r+k'} - eX_{i,i+k'-k}, \qquad e = Y_{r,r+k}.$$

Since $X_{is} = X_{i,i+k'-k}$, and we may assume this is non-zero, we have by (H2),

$$k' - k \in ([0, n-s) \cap 4\mathbf{Z}) \cup ([n-s, n) \cap 2\mathbf{Z}) \cup \{n\}. \tag{7}$$

Now we check the hypotheses (H1), (H3), (H4), and (H5) for Y'.

Verification of (H1): Is $Y'_{r,r+m} = 1$? Equations (6) and (7) cannot both hold when $k' = m$, therefore $Y'_{r,r+m} = Y_{r,r+m} = 1$.

Verification of (H3): First we show $Y'_{rj} = 0$ if $j < r$. Since $k = i - r \in [0, m)$, we see $j < r \leq i$, and so $X_{ij} = 0$. Then $Y'_{rj} = Y_{rj} = 0$. Next, we show Y'_{rj} is even when $j \neq m + r$. This is because $Y'_{rj} = Y_{rj} - eX_{ij}$, e is even, and Y_{rj} is even.

Verification of (H4): Let $0 \leq k' < m - s$. Then $k' - k < m - s$, so $k' = k \pmod 4$ and $k \leq k' < m - s$ by (7). By (6), $4|k$ and $4|e$. Since $k' = k \pmod 4$, $4|k'$. Then $Y'_{r,r+k'} \equiv Y_{r,r+k'} \equiv 0 \pmod 4$, as required.

Verification of (H5): Let $m - s \leq k' < m + n - 2s$ and $k' \neq m$. We will show (H5) holds for $Y'_{r,r+k'}$. Since $Y'_{r,r+k'} = Y_{r,r+k'} - eX_{i,i+k'-k}$ and (H5) holds for $Y_{r,r+k'}$, it suffices to show

$$eX_{i,i+k'-k} = \begin{cases} 0 \pmod 2 & \text{if } k' = 2 \pmod 4, \\ 0 \pmod 4 & \text{if } k' = 0 \pmod 4, \text{ or if } k' \text{ is odd and } r + k' > m, \\ 0 \pmod 8 & \text{if } k' \text{ is odd and } r + k' \leq m. \end{cases} \tag{8}$$

This is certainly true when $k' = 2 \pmod 4$ since e is always even, so assume $k' \neq 2 \pmod 4$. We claim $4|k$. If not, then by (6), $k = 2 \pmod 4$ and $k \geq m - s$, so $k' - k < (m + n - 2s) - (m - s) \leq n - s$. By (7), $k' - k \in [0, n - s) \cap 4\mathbf{Z}$. So $k' = k = 2 \pmod 4$, contradicting our assumption that $k' \neq 2 \pmod 4$. This proves the claim that $4|k$. By (6), $4|e$. Thus, (8) holds except possibly when k' is odd and $r + k' \leq m$. By (6) and (7), k' odd implies $k' - k = n$, in which case $r + k' > m$. This proves (H5). ∎

References

[1] O. Ahmadi and A. Menezes, *On the number of trace-one elements in polynomial bases for* $\mathbb{F}_{2^n}$, *preprint*, available at http://www.cacr.math.uwaterloo.ca∼ajmeneze/research.html

[2] H. Fredricksen, A. W. Hales, and M. M. Sweet, *A generalization of Swan's theorem*, Math. Computation, 321-331, 1986

[3] A. W. Hales and D. W. Newhart, *Irreducibles of tetranomial type*, in J. No, H. Song, T. Helleseth, and P. Kumar, editors, *Mathematical Properties of Sequences and Other Combinatorial Structures*, Boston, 2003, Kluwer Academic Publishers

[4] R. G. Swan, *Factorization of Polynomials over Finite Fields*, *Pacific J. Math* **12**, 1962, 1099–1106

[5] B. L. van der Waerden, *Algebra*, Volume I, (first published with the title *Moderne Algebra* in 1930-31), Springer: New York, 1991